STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: LAN Backup and Archiving Plan

Product ID: ENT-NET-010

Effective Date: March 11, 1998

Approved: LOIS MENZIES, Director

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

This policy refers to local area networks which includes file servers and workstations.

For the purposes of this policy, the following definitions apply:

Backup: A disk or tape on which important data is duplicated for the purpose of safety. Should the original stored information become corrupt or lost, the information can be retrieved from the backup. A backup allows for recovery of data in the case of a disaster.

Electronic Archiving: The act of storing electronic files for future retrieval. If an electronic document is ever needed in the future, it should be archived. Only select documents should be archived.

Archives: Those records that have been determined to have sufficient historical or other value to warrant their permanent preservation and that have been transferred to the State Archive's custody.

Each agency must have a written backup plan including a backup schedule, backup process and a list of mission critical applications. Agencies should consider their current electronic archiving process (the storing of files for future retrieval, not the process of sending documents to the State Archives) while developing their backup plan. Agencies cannot use the backup process as an electronic archiving method; a separate electronic archiving process and plan must be developed. The backup plan must be reviewed annually and periodically tested by the agency network administrator. Each agency must maintain a notification list of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency.

At a minimum, modified data on file servers must be backed up at the end of each work day and a full system backup must be performed at least once a week. Mission critical data should be backed up, regardless of where it resides. On a monthly basis at least one full backup must be stored off-site.

Agencies must retain backup tapes for no longer than thirty (30) days unless this retention schedule is extended by an agency head to address a compelling business need for the agency. The backup tapes must be erased and reused, or destroyed, after thirty (30) days.

Weekly backups of the NetWare Directory Structure (NDS) will be completed by the Information Technology Services Division, Department of Administration. Network Administrators must contact the ITSD Service Desk for NDS restorations.

A. Background - History On The Creation Of Or Changes To This Policy

This policy was originally created by the NetWare Managers Group Policy Committee. It was then modified to reflect concerns of document and email retention and was reviewed by an ad hoc committee created by Lois Menzies, Director of the Department of Administration. The Information Technology Advisory Council reviewed and approved this policy.

B. Guidelines - Recommendations, Not Requirements

It is recommended agencies maintain a list of hardware specifications for all critical systems to insure appropriate replacement hardware can be provided in case of a disaster. Network administrators should be trained in the use of current backup hardware, software and policies. Agencies should insure users are trained in proper workstation backup procedures.

It is also recommended agencies maintain a set of diskettes containing an emergency recovery configuration and backup software both on-site and off-site. Agencies should test the viability of these diskettes to recover the system and load the backup software in order to perform a full system restore.

A consideration for an agency's electronic archiving plan is to designate certain directories or drives for electronic archiving. These directories or drives should not contain email or documents which are considered temporary. Another consideration for an agency's electronic archiving plan is to include a migration plan for transferring data from one media to another as technology changes.

References - Laws, rules, standard operating procedures and applicable policies

C. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-505(2), MCA
- 2-15-112, MCA
- 2-17-514(1) – Enforcement

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-114, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-NET-010
Proponent:	LOIS MENZIES, Director
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	March 11, 1998
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.